УДК 512.624.95 + 517.772

к.т.н. Чевардін В.Є. (ВІТІ НТУУ „КПІ”)
Ізофатов Д.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Сокіл Г.В. (ПНТУ)

РЕАЛІЗАЦІЯ ГЕНЕРАТОРА DUAL_EC_DRBG НА ОСНОВІ ПОДВІЙНОГО СКАЛЯРНОГО МНОЖЕННЯ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ ЗІ ЗМІННИМИ ПАРАМЕТРАМИ

Представлені результати аналізу обчислювальної складності генераторів псевдовипадкових послідовностей на основі еліптичних кривих, рекомендованих сучасними стандартами. Запропоновано програмну реалізацію генератора Dual_EC_DRBG зі змінними параметрами еліптичної кривої. Отримані реалізації генератора Dual_EC_DRBG скоротили обчислювальну складність перетворень в 2 – 3 рази.

Чевардин В.Е., Изофатов Д.А., Сокол Г.В. Реализация генератора Dual_EC_DRBG на основе двойного скалярного умножения точек эллиптической кривой с переменными параметрами. *Представлены результаты анализа вычислительной сложности генераторов псевдослучайных последовательностей на основе эллиптических кривых, рекомендованных современными стандартами. Предложена программная реализация генератора Dual_EC_DRBG с переменными параметрами эллиптической кривой. Полученные реализации генератора Dual_EC_DRBG сократили вычислительную сложность преобразований в 2 – 3 раза.*

V. Chevardin, D. Izofatov, G. Sokol The implementation of the Dual_EC_DRBG generator based on a double scalar multiplication of elliptic curve points with variable parameters. *The analysis results of computational complexity of random bit generators based on elliptic curves recommended by modern standards are shown in this work. The program implementation of the Dual_EC_DRBG generator with variable parameters of the elliptic curve is proposed. The resulting implementations of the Dual_EC_DRBG generator reduced computational complexity of the transformation in 2– 3 times.*

Ключові слова: *випадкова послідовність, генератор псевдовипадкових послідовностей, еліптична крива, обчислювальна складність.*

1. Формулювання задачі

Сучасний розвиток суспільства вже неможливий без використання надійної та захищеної інформаційно-телекомунікаційної складової. Враховуючи важливість криптографічно стійких перетворень для забезпечення високої ефективності систем захисту інформації, основним етапом розробки нових та вдосконалення існуючих криптосистем є аналіз ефективності (криптографічна стійкість / обчислювальна складність) генераторів псевдовипадкових послідовностей (ПВП).

Результати останніх досліджень в області алгоритмів генерації ПВП показали поступове проникнення відомих теоретико-складних задач математики практично в усі напрямки розвитку сучасних криптографічних систем захисту інформації. Як показали проведені дослідження та відомі результати [1 – 12], алгоритми генерації ПВП на основі еліптичних кривих (ЕК) є одними з перспективних генераторів, що мають теоретично доведену стійкість, які дозволяють довести еквівалентність криптографічної стійкості генератора та складності задачі дискретного логарифмування в групі точок ЕК. Результатом багатьох досліджень є поява нового стандарту [13], який містить рекомендації щодо генерації ПВП на основі подвійного скалярного множення точок еліптичної кривої. В останні роки на адресу цього стандарту виникає немало критики [14, 15], яка присвячена досить великій обчислювальній складності генератора, а також рекомендованим параметрам кривої, які зафіксовані для будь-якого використання.

В зв’язку з чим, актуальним питанням постає аналіз шляхів зниження обчислювальної складності криптографічних перетворень, які використовуються в сучасних генераторах ПВП на основі еліптичних кривих.

2. Аналіз відомого підходу щодо генерації ПВП на еліптичних кривих

Відомими результатами оцінки криптографічної стійкості генератора Dual_EC_DRBG є роботи [14, 15], в яких вказані слабкі місця алгоритму, пов’язані з фіксованими

загальносистемними параметрами генератора. Дійсно, вимога розробників щодо використання тільки тих еліптичних кривих, які затверджені у стандарті, є сумнівною.

Для побудови даного генератора рекомендована звичайна несуперсингулярна крива у формі (1):

$$y^2 = (x^3 - 3x + b) \bmod p, \qquad (1)$$

де $b \in F_p$, p – велике просте число.

Використання коефіцієнту a = –3 дозволяє представляти точки кривої у формі Якобі, що використовує операції над точками кривої зі зниженою обчислювальною складністю. Для практичних цілей обрані криві над скінченними полями простої характеристики з розрядністю 256, 384 та 521 біт, параметри яких зафіксовані. Наприклад, для P-256 параметри кривої мають наступні значення:

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951;

n = 115792089210356248762697446949407573529996955224135760342422259061068512044369;

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b.

Це не дозволяє використовувати альтернативні криві для генерації ПВП, які мають кращі характеристики щодо швидкості операцій над точками. Також, користувач не може змінити параметри кривої у випадку компрометації генератора з такими параметрами. Можливість змінити базові точки кривої не дає змогу встановлювати повністю власні параметри криптосистеми, а також не дозволяє використовувати такий генератор на одній платформі з відомими криптосистемами: цифровим підписом на еліптичних кривих над полем 160 біт, алгоритмами генерації Діффі-Хеллмана на еліптичних кривих тощо. Це потребує додаткових витрат на програмно-апаратну реалізацію генераторів ПВП на еліптичних кривих. В зв’язку з цим, **метою** роботи є реалізація генератора Dual_EC_DRBG з використанням стандартизованих еліптичних кривих зі змінними параметрами для розширення можливостей користувачів, а також для зниження обчислювальної складності перетворень під час генерації ПВП.

3. Реалізація генератора Dual_EC_DRBG

Загальна модель механізму генерації DRBG наведена на рис. 1. Згідно стандартизованої моделі (рис. 1) використовується три рівня перетворень (j = 1, 2, 3) для генерації ПВП.

Великим стрілками вказаний шлях секретних параметрів DRBG, тобто з урахуванням усіх загальносистемних параметрів секретність генератора забезпечується наступним чином:

– рівень j = 1: з використанням джерела ентропії створюється секретна початкова ентропія E, яка потрапляє до блока генерації seed;

– рівень j = 2: seed потрапляє до блока формування параметра si на основі використання односпрямованої функції (шифр або геш-функція), на виході з’являється значення si, яке також вважається секретним, та подається до наступного блока;

– рівень j = 3: послідовність si обробляється з використанням другої односпрямованої функції та відправляється на вихід генератора;

– вихід генератора, згідно стандарту, перевіряється спеціальною функцією на випадок зациклення генератора (функція тестування ПВП), тобто на випадок створення вироджених послідовностей з нулів або одиниць.

В якості односпрямованих функцій використовують один тип перетворень, що є принципово відмінним для усіх генераторів DRBG та забезпечує відповідний рівень криптографічної стійкості. Для випадку реалізації DRBG на основі еліптичних кривих в якості односпрямованої функції використовують операцію скалярного множення точки еліптичної кривої. Запропоновано також інші варіанти використання: спарювання точок кривої [10], ізоморфні трансформації точок кривої [11, 12].

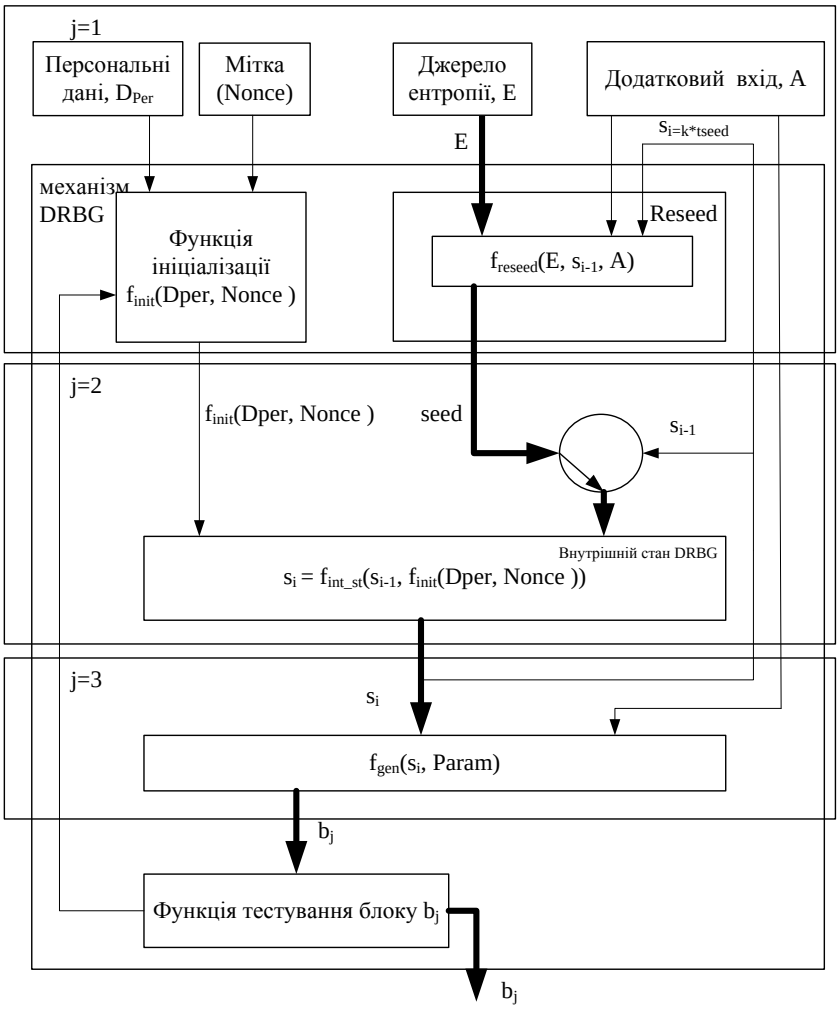

Рис. 1. Загальна модель механізму DRBG

4. Реалізація Dual_EC_DRBG та аналіз обчислювальної складності

Розглянемо деякі варіанти побудови генератора Dual_EC_DRBG з використанням відомих кривих Коблиця та Вейєрштрасса над простими та розширеними полями Галуа. Програмна реалізація генераторів випробувалась з використанням програмно-апаратного комплексу на базі Asus-P6200 (Intel™ Pentium™ Westmere™ Arrandale™ CPU-P6200 з частотою 2133000000 Hz; набір інструкцій: x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3; оперативна пам’ять: DDR3-1066 3885 Mb) з використанням 32-бітного компілятора. Під час реалізації відомих криптографічних алгоритмів та відомих генераторів ПВП використовувались останні результати вдосконалення алгоритмів, з урахуванням доступних імплементацій для обраної праграмно-апаратної платформи. В таблиці 1 наведені результати оцінки обчислювальної складності алгоритмів генерації ПВП.

Так, криві: K-163, K-233, K-283, K-409, K-571 є кривими Коблиця, криві: B-163, B-233, B-283, B-409, B-571 є кривими Вейєрштрасса. Усі криві представлені в таблиці 1 є кривими, рекомендованими для практичної реалізації згідно стандартів: FIPS PUB 186-3, SEC 1, ANSI X9.62, IEEE 1363-2000, ISO/IEC 14888-3. Криві: U-163, U-239, U-307 є кривими, рекомендованими згідно стандарту ДСТУ 4145-2002.

Порівняльна оцінка алгоритмів генерації ПВП на основі перетворень в групі точок еліптичної кривої наведена на рис. 2.

Таблиця 1

Часові та швидкісні показники для генераторів ПВП, побудованих на основі скалярного множення точок кривих Коблиця та Вейєрштрасса

Алгоритм генерації ПВП	Рівень безпеки (NIST SP 800-57 Частина 1) (біт)	Утилізація ядра процесора, *Utl* (%)	Пропускна спроможність алгоритму, *Rate* (байт/сек)	Обчислювальна складність, *Per* (cpb)
Dual_EC_DRBG(P-256)	128	56	5413	220668,5
Dual_EC_DRBG(P-384)	192	56	3368	354655,5
Dual_EC_DRBG(P-521)	256	56	2153	554797,5
Dual_EC_DRBG(K-163)	80	56	16816	71032,0
Dual_EC_DRBG(K-233)	112	56	14643	81573,0
Dual_EC_DRBG(K-283)	128	56	12670	94276,0
Dual_EC_DRBG(K-409)	192	56	8361	142863,0
Dual_EC_DRBG(K-571)	256 (272_{real})	56	6037	197859,5
Dual_EC_DRBG(B-163)	80	56	9177	130160,0
Dual_EC_DRBG(B-233)	112	56	7223	165371,5
Dual_EC_DRBG(B-283)	128	56	5822	205166,5
Dual_EC_DRBG(B-409)	192	56	3258	366629,5
Dual_EC_DRBG(B-571)	256 (272_{real})	56	2201	542698,5
Dual_EC_DRBG(U-163)	80	56	9177	130160,0
Dual_EC_DRBG(U-239)	112	56	14673	81406,5
Dual_EC_DRBG(U-307)	128 (144_{real})	56	5336	223853,0

За результатами дослідження обчислювальної складності алгоритм генерації ПВП Dual_EC_DRBG (K-163) на основі перетворень в групі точок еліптичної кривої над полем 163 біти володіє найменшою обчислювальною складністю. Dual_EC_DRBG (K-163) реалізований з використанням кривої Коблиця, що пояснює виграш в обчислювальній складності над іншими генераторами.

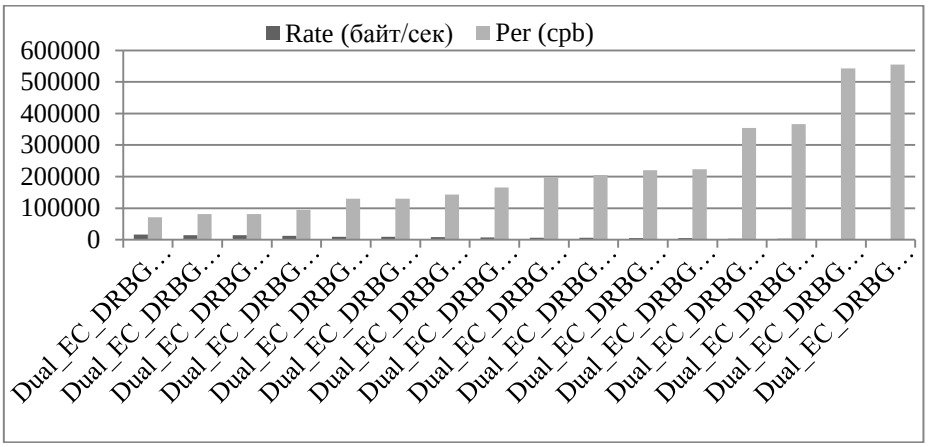

Рис. 2. Оцінка обчислювальної складності генераторів Dual_EC_DRBG, побудованих на основі перетворень в групі точок еліптичної кривої

Результати дослідження обчислювальної складності генераторів ПВП показали, що використання кривих Коблиця над полями 571 біт має кращі показники, як пропускної спроможності алгоритму *Rate*, так і обчислювальної складності *Per* у порівнянні з Dual_EC_DRBG (P-521). Генератор ПВП Dual_EC_DRBG (B-283), побудований на основі

кривих затверджених міжнародним стандартом, також дозволяє отримати кращі показники обчислювальної складності у порівнянні з Dual_EC_DRBG (P-256).

Розділимо усі генератори, які досліджувались, на категорії стійкості: 80, 112, 128, 192, 256 біт. Якщо згрупувати усі генератори за критерієм стійкості, яка забезпечується ними, можна отримати різницю обчислювальної складності генераторів, побудованих на еліптичних кривих (рис. 3).

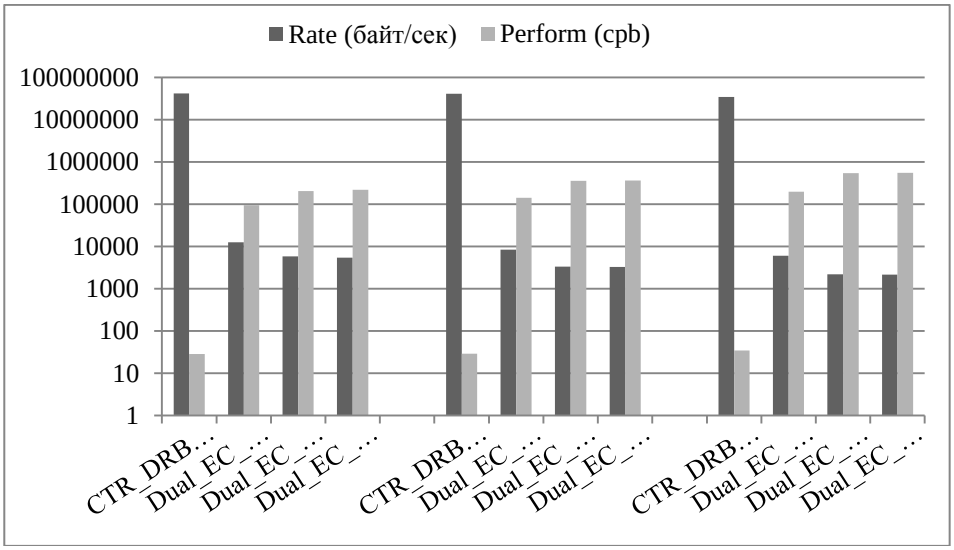

Рис. 3. Результати порівняльної оцінки обчислювальної складності генераторів ПВП на основі еліптичних кривих

Побудова генератора Dual_EC_DRBG на основі кривої B-283 дозволила збільшити криптографічну стійкість генератора DRBG еквівалентну збільшенню характеристики поля на 27 біт, а також отримати незначне зменшення обчислювальної складності перетворень в 1,07 рази. Побудова генератора Dual_EC_DRBG на основі кривої K-283 дозволила збільшити криптографічну стійкість генератора Dual_EC_DRBG (P-256) еквівалентну збільшенню характеристики поля на 27 біт, а також отримати зменшення обчислювальної складності перетворень в 2,34 рази. Побудова генератора Dual_EC_DRBG на основі кривої K-409 дозволила збільшити криптографічну стійкість генератора Dual_EC_DRBG (P-384) еквівалентну збільшенню характеристики поля на 25 біт, а також отримати зменшення обчислювальної складності перетворень в 2,48 рази.

Побудова генератора Dual_EC_DRBG на основі кривої B-571 дозволила збільшити криптографічну стійкість генератора Dual_EC_DRBG (P-521) еквівалентну збільшенню характеристики поля на 50 біт, а також отримати незначне зменшення обчислювальної складності перетворень в 1,02 рази. Побудова генератора Dual_EC_DRBG (K-571) на основі кривої K-571 дозволила збільшити стійкість генератора Dual_EC_DRBG (P-521) еквівалентну збільшенню характеристики поля на 50 біт, а також отримати зменшення обчислювальної складності перетворень в 2,8 рази.

Висновки

Таким чином, перехід від запропонованих стандартом [13] еліптичних кривих до інших кривих, рекомендованих для криптографічних цілей сучасними стандартами FIPS PUB 186-3, SEC 1, ANSI X9.62, IEEE 1363-2000, ISO/IEC 14888-3, ДСТУ 4145-2002, дозволив зменшити обчислювальні витрати на криптографічні перетворення під час генерації псевдовипадкових послідовностей у 2 – 3 рази.

Використання змінних параметрів для побудови сучасних генераторів ПВП на еліптичних кривих дозволило надати можливість користувачам обирати власні параметри генерації ПВП та мати більше число реалізацій генераторів цього класу.

Слід зауважити, що реалізація генераторів ПВП на еліптичних кривих все ж таки залишається складною задачею у порівнянні з іншими генераторами на основі блочних шифрів та алгоритмів гешування, що викликає потребу в подальших дослідженнях, направлених на використання більш ефективних підходів щодо зниження обчислювальної складності перетворень під час генерації ПВП на еліптичних кривих.

ЛІТЕРАТУРА

1. Kaliski Jr. B. S. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84 – 103.

2. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. – 1989, pp. 12 – 24.

3. Burton S. One-Way Permutations on Elliptic Curves / Burton S. Kaliski, Jr. // Journal of Cryptology (1991) International Association for Cryptologic Research. – 1991, pp. 187 – 199.

4. Shparlinski I. E. On the Naor-Reingold pseudo-random function from elliptic curves, Applicable Algebra in Engineering, Communication and Computing 11 (2000), pp. 27 – 34.

5. Потий А.В. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / Потий А.В., Орлова С.Ю., Гриненко Т.А. // Вип. 2. – Київ. – 2001 р. – С. 206 – 213.

6. Горбенко И.Д. Сложность арифметических операций в группах точек эллиптических кривых для криптографических операций / И.Д. Горбенко , С.И. Збитнев , А.А. Поляков // Всеукр. межвед. науч.-техн. сб. Радиотехника. – Вып. 119.– 2001.– С. 51 – 55.

7. Гриненко Т.А. Методы формирования псевдослучайных последовательностей в группах точек эллиптических кривых / Т.А. Гриненко, С.И. Збитнев, Д.В. Мялковский // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2002. – Вып. 119. – С. 119 – 123.

8. Beelen P. Pseudorandom sequences from elliptic curves / Beelen P., Doumen J. // Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, 2002, pp. 37 – 52.

9. Lange T. Certain exponential sums and random walks on elliptic curves / Lange T., Shparlinski I. E. // Canadian Jornal of Mathematics 57. – 2005, pp. 338 – 350.

10. Горбенко І.Д. Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / Горбенко І.Д., Шапочка Н.В., Погребняк К.А. // Журнал „Прикладная радиоэлектроника” 2010. – № 3. Харьков – 2010. – С. 386 – 394.

11. Бессалов А. В. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой / Бессалов А. В., Чевардин В. Е. // Прикладная радиоэлектроника: науч.-техн. Журнал. – 2012.–Том 11, № 2. – С. 234 – 237.

12. Чевардін В. Є. Генераторы псевдослучайных последовательностей на основе теоретикосложностных задач математики / В.Є. Чевардін // Збірник наукових праць ВІТІ НТУУ „КПІ”, Випуск № 1, Київ, ВІТІ НТУУ „КПІ”. – 2012 р. – С.125 – 134.

13. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012.

14. Schoenmakers B. Cryptanalysis of the Dual Elliptic Curve Pseudorandom sequences from elliptic curves / Schoenmakers B., Sidorenko A. // 29 may 2006.

15. Зайцева Н.Ю. Атака розпізнавання на генератори псевдовипадкових послідовностей на основі еліптичних кривих / Зайцева Н.Ю., Завадська Л.О. // Теоретичні і прикладні проблеми фізики, математики та інформатики. – Збірка тез доповідей. ВПІ ВПК „Політехніка”. – Київ. – 2012. – С. 238 – 239.